

Ihr Laptop – mit Sicherheit?

Agenda

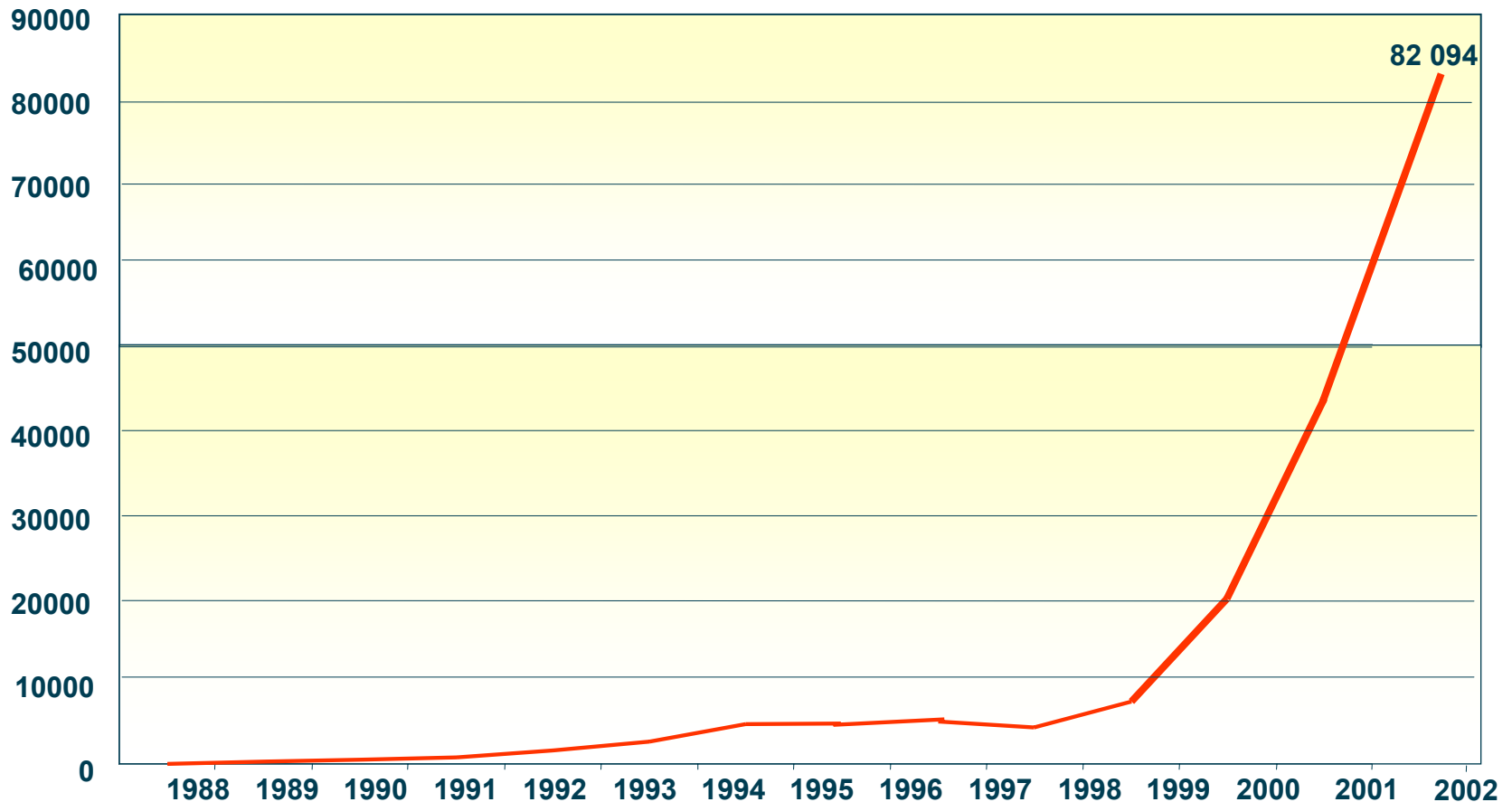
- Was bedroht Sie und Ihren Laptop?
- Legen Sie Ihren Laptop an die Kette
- Ihr Laptop – mit Sicherheit!



Was bedroht Sie und Ihren Laptop?

Was bedroht Sie und Ihren Laptop?

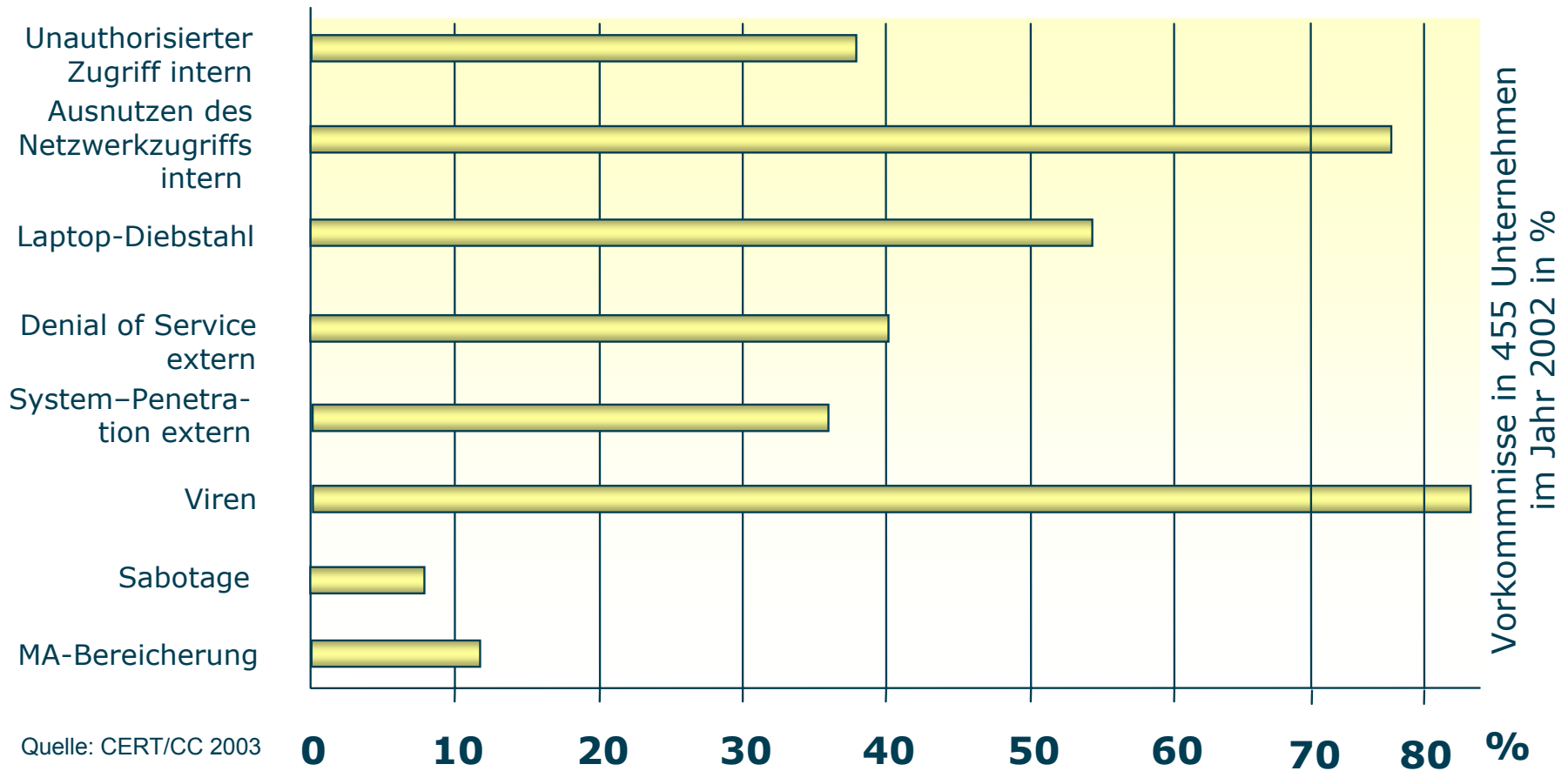
- Gemeldete Sicherheitsprobleme beim CERT (Computer Emergency Response Team)



Quelle: CERT/CC -- http://www.cert.org/stats/cert_stats.html

Was bedroht Sie und Ihren Laptop?

- Die Gefahren im Überblick





Legen Sie Ihren Laptop an die Kette

Legen Sie Ihren Laptop an die Kette



- Auf Reisen
 - Lassen Sie Ihren Laptop nicht unbeaufsichtigt!
 - Weder im Hotel, noch im Restaurant, noch im Zug
 - Lassen Sie Ihren Laptop nicht sichtbar im Auto liegen!
 - Schließen Sie ihn im Kofferraum ein.
 - Der Kofferraum ist kein Aufenthaltsort für die Nacht.
 - Sichern Sie Ihren Laptop in fremden Räumen!
 - Verschließen Sie fremde Räume auch bei kurzzeitigem Verlassen.
 - Schalten Sie Ihren Laptop aus, wenn Sie den Raum für längere Zeit verlassen.
 - Verhindern Sie die unerlaubte Nutzung Ihres Laptops. Verwenden Sie ein Boot-Passwort.

Legen Sie Ihren Laptop an die Kette



- Auf Reisen
 - Lassen Sie Ihren Laptop in Hotelräumen nicht sichtbar liegen!
 - Verschießen Sie Ihren Laptop in einem Schrank. Das behindert Gelegenheitsdiebe.
 - Heutige Laptops oder PC-Zubehör können Sie anketten.
 - Ihr Laptop kann dann nur mit Hilfe von Werkzeug gestohlen werden.

Legen Sie Ihren Laptop an die Kette



- Im Büro
 - Ihr Laptop ist besonders leicht zu transportieren und zu verbergen.
 - Verschließen Sie Ihren Laptop außerhalb der Nutzungszeit in einem Schrank.
 - Diebstahl-Sicherungen machen dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist.
 - Sichern Sie sowohl Ihren Laptop, als auch das Zubehör.

Legen Sie Ihren Laptop an die Kette



- Zu Hause
 - Für den häuslichen Arbeitsplatz ist die Nutzung eines Arbeitszimmers wünschenswert.
 - Verschließen Sie bei Abwesenheit das Arbeitszimmer, damit Laptop, Dokumente und Datenträger gesichert sind.
 - Verschließen Sie Fenster und Türen!
 - Verschließen Sie Balkon-, Terrassentüren und Fenster in den Zeiten, in denen Sie den Raum nicht nutzen.
 - Verschließen Sie den Laptop über Nacht oder wenn Sie das Haus verlassen!
 - Verschließen Sie Ihren Laptop in einem Schrank. Das behindert Gelegenheitsdiebe.

Legen Sie Ihren Laptop an die Kette



- **Kontrollfragen**

- Werden die Benutzer von Laptops auf die geeignete Aufbewahrung hingewiesen?
- Wie werden Laptops in den Büros aufbewahrt?
- Ist der Mitarbeiter darauf hingewiesen worden, dass Laptop, Dokumente und Datenträger zu Hause verschlossen aufzubewahren sind?

- **Verantwortlich für Initiierung:** **IT-Leiter, IT-Sicherheitsmanagement**
- **Verantwortlich für Umsetzung:** **IT-Benutzer**



Ihr Laptop – mit Sicherheit!

Ihr Laptop – mit Sicherheit!

- Verwenden Sie ein Boot-Passwort
 - Aktivieren Sie das Boot-Passwort Ihres Laptops.
 - Ihr Laptop wird erst nach der Eingabe des Boot-Passwortes hochgefahren.
 - Wenn Ihr Laptop keine Passwortroutine besitzt, sollten Sie Ihre sensiblen Daten verschlüsseln.
 - Können Ihre sensiblen Daten nicht verschlüsselt werden, speichern Sie diese nicht auf Ihrem Laptop.



Enter old Power-On Password: *****

Enter new Power-On Password:

Enter new Power-On Password:

Enable Password to Power-on

OK

Cancel

Ihr Laptop – mit Sicherheit!

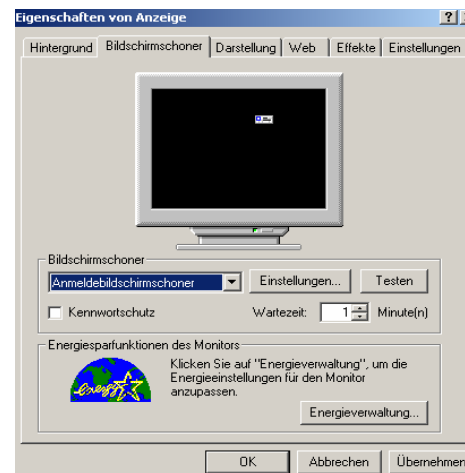
- Verwenden Sie "starke" Passwörter
 - Leicht zu merken - schwer zu erraten
 - Mindestens 7 Zeichen lang
 - Mindestens ein Sonderzeichen oder eine Zahl
 - Voreingestellte Passwörter sofort ändern
 - Alte Passwörter nicht wieder verwenden
 - Ungeeignet sind: Namen, Personal-, Abteilungsnummern, Wiederholung der Benutzerkennung, benachbarte Zeichen der Tastatur,...



So ein Tag, so wunderschön wie heute

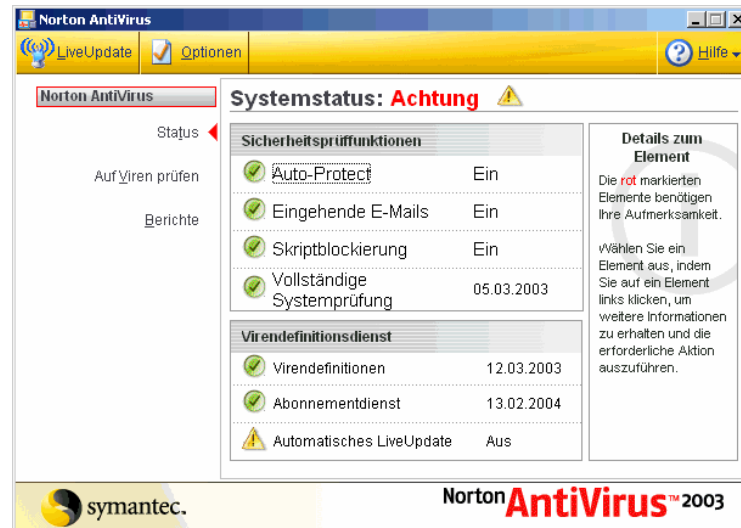
Ihr Laptop – mit Sicherheit!

- Bildschirmsperre
 - Nutzen Sie die Bildschirmsperre Ihres Laptops. Diese sollte sich automatisch nach einem vorgegebenen Inaktivitäts-Zeitraum (z.B. 15 min) aktivieren.
 - Aktivieren Sie Ihre Bildschirmsperre, wenn sie den Arbeitsplatz für kurze Zeit verlassen.
 - Melden Sie sich bei längerer Abwesenheit beim System ab.



Ihr Laptop – mit Sicherheit!

- Einsatz eines Viren-Scanners
 - Installieren Sie auf Ihrem Laptop einen Viren-Scanner, der beim Systemstart automatisch aktiv wird.
 - Die regelmäßige Aktualisierung und die Parametrisierung des Viren-Scanners ist durch das IT-Sicherheitsmanagement Ihres Unternehmens definiert.

Norton AntiVirus

Systemstatus: **Achtung** ⚠

Sicherheitsprüffunktionen

Auto-Protect	Ein
Eingehende E-Mails	Ein
Skriptblockierung	Ein
Vollständige Systemprüfung	05.03.2003

Virendefinitionsdienst

Virendefinitionen	12.03.2003
Abonnementdienst	13.02.2004
Automatisches LiveUpdate	Aus

Details zum Element

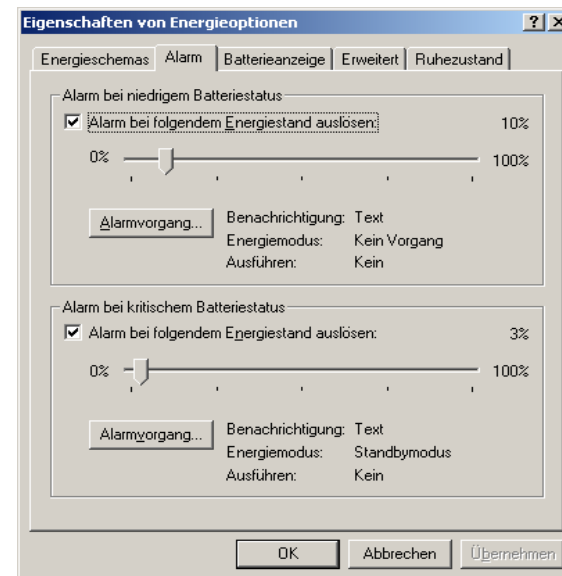
Die rot markierten Elemente benötigen Ihre Aufmerksamkeit.

Wählen Sie ein Element aus, indem Sie auf ein Element links klicken, um weitere Informationen zu erhalten und die erforderliche Aktion auszuführen.

symantec. Norton **AntiVirus**™ 2003

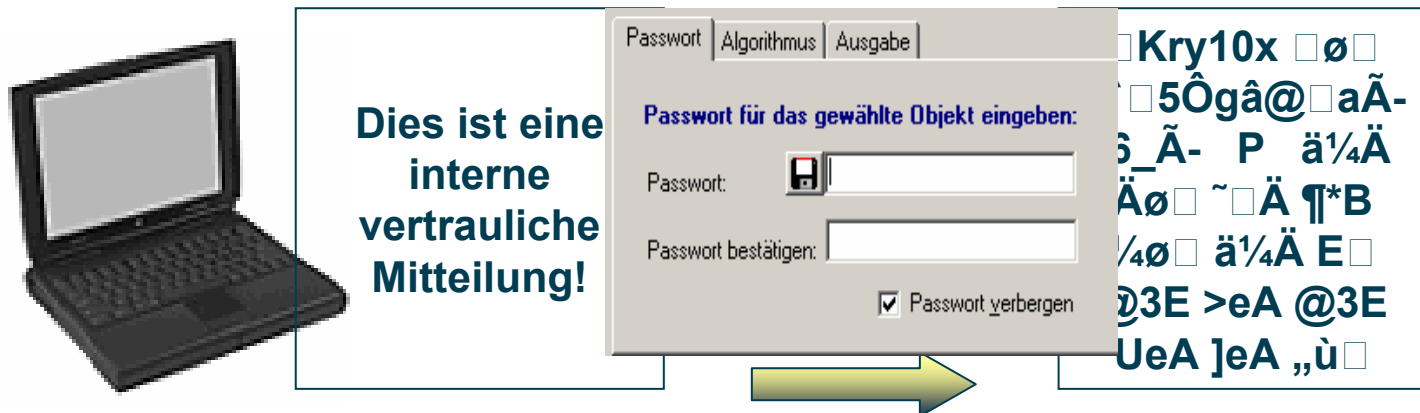
Ihr Laptop – mit Sicherheit!

- Energieversorgung im mobilen Einsatz
 - Vermeiden Sie Datenverlust im Batteriebetrieb. Beachten Sie die Energiewarnanzeigen, -signale Ihres Laptops.
 - Sichern Sie die aktuell verarbeiteten Daten in kurzen Zeitabständen auf die Festplatte.
 - Nutzen Sie die automatische Datensicherung in den Standardprogrammen.



Ihr Laptop – mit Sicherheit!

- Einsatz eines Verschlüsselungsprogramms
 - Nutzen Sie für Ihren Laptop ein Verschlüsselungsprogramm. Damit verhindern Sie, dass bei einem Diebstahl sensible Daten gelesen werden können.
 - Marktgängige Produkte verschlüsseln einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte.
 - Auch bei den Verschlüsselungsprogrammen sollten Sie ein "starkes" Passwort verwenden.



Dies ist eine interne vertrauliche Mitteilung!

Passwort | Algorithmus | Ausgabe

Passwort für das gewählte Objekt eingeben:

Passwort:

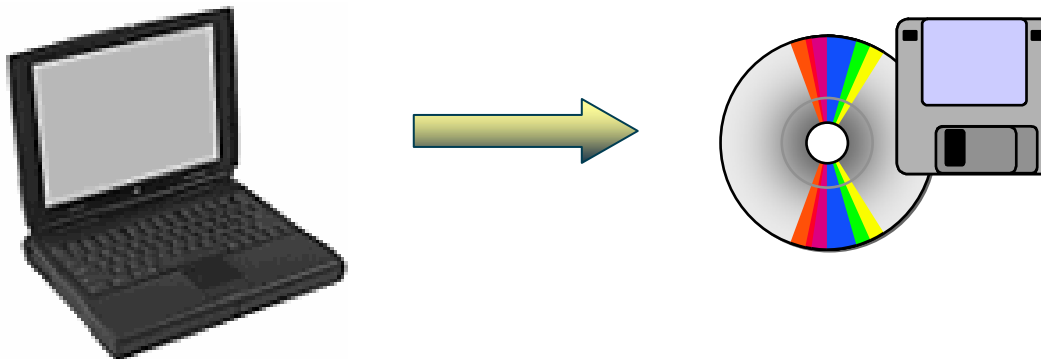
Passwort bestätigen:

Passwort verbergen

Kry10x ø
5Ôgâ@aÃ-
s_Ã- P ä¼Ä
Äø ~Ä ¶*B
¼ø ä¼Ä E
D3E >eA @3E
UeA]eA „ù

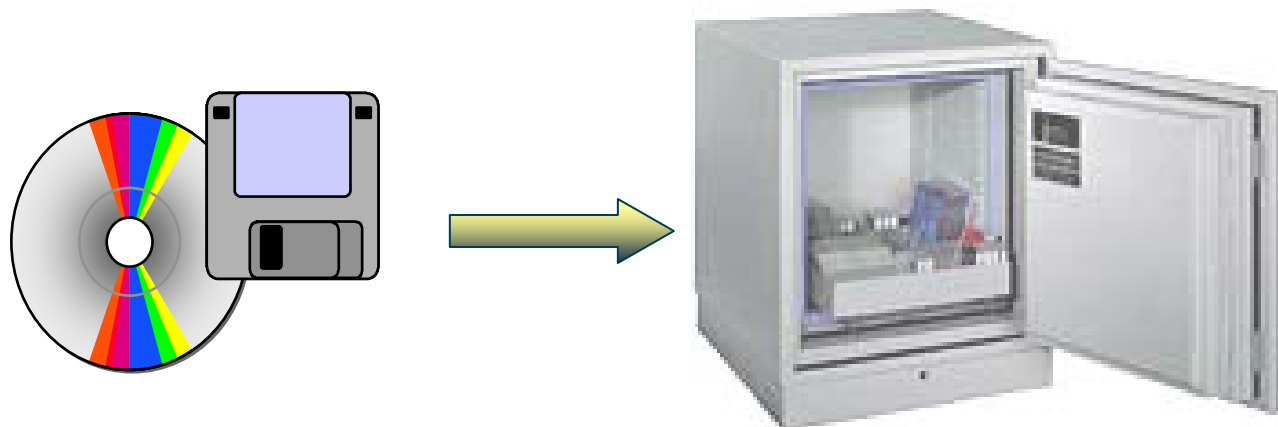
Ihr Laptop – mit Sicherheit!

- Datensicherung auf externen Datenträgern
 - Verschlüsseln Sie Ihre Datensicherung. Kommen unverschlüsselte externe Datenträger abhanden, besteht die Gefahr, dass sensitive Daten "in falsche Hände" kommen.
 - Verwenden Sie externe Datenträger mit einer angemessenen Speicherkapazität.
 - Bewahren Sie Ihre Datenträger und Ihren Laptop getrennt voneinander auf.



Machen Sie Ihren Laptop fit

- Aufbewahrung der Backup-Datenträger
 - Bewahren Sie Ihre Backup-Datenträger getrennt vom Laptop, in einem anderen Brandabschnitt, auf.
 - Verhindern Sie unbefugten Zugriff auf Ihre Datenträger. Nur so kann Diebstahl ausgeschlossen werden.
 - Stellen Sie einen ausreichend schnellen Zugriff im Bedarfsfall sicher.



Machen Sie Ihren Laptop fit

- Datensicherung über temporäre Netzverbindungen
 - Besteht die Möglichkeit, Ihren Laptop regelmäßig an das Unternehmens-Netz anzuschließen, erfolgt die Sicherung Ihrer lokalen Daten über die Netzanbindung.
 - Ihr Vorteil ist, dass Sie keine Datenträger verwalten und auch kein spezielles Laufwerk mitführen müssen.



Machen Sie Ihren Laptop fit

- Kontrollfragen

- Werden Boot-Passwörter für Laptops benutzt?
- Werden "starke" Passwörter benutzt?
- Wird die Bildschirmsperre konsequent eingesetzt?
- Wird ein Viren-Scanner eingesetzt?
- Wann wird der eingesetzte Viren-Scanner aktualisiert?
- Werden die Benutzer im Umgang mit dem Verschlüsselungsprogramm geschult?
- Werden Daten und Schlüssel getrennt aufbewahrt?
- Werden alle Daten, die auf dem Laptop lokal gespeichert werden, regelmäßig gesichert?
- Wo werden die Datenträger der Datensicherung eines jeden Laptops aufbewahrt?

- Verantwortlich für Initiierung: IT-Leiter
- Verantwortlich für Umsetzung: IT-Benutzer

Machen Sie Ihren Laptop fit

- Weitere organisatorische Maßnahmen
 - Schulung der Benutzer
 - Datenträgerverwaltung
 - Regelungen für Wartungs- und Reparaturarbeiten
 - Nutzungsverbot nicht freigegebener Software
 - Überprüfung des Software-Bestandes
 - Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
 - Hinterlegen des Passwortes
 - Herausgabe einer PC-Richtlinie
 - Einführung eines PC-Checkheftes
 - Geregelter Übergabe und Rücknahme eines Laptops

 - Verantwortlich für Initiierung: IT-Leiter
 - Verantwortlich für Umsetzung: IT-Leiter, Administrator, IT-Benutzer

Wir freuen uns über Ihr Feedback



Network Training and Consulting GmbH
Weidenauer Straße 15
57078 Siegen
siegen@networktraining.de

Network Training and Consulting Südwest GmbH
Gutenbergstraße 13
70771 Leinfelden-Echterdingen
stuttgart@networktraining.de

Bundesweite Infoline: 0180 11 77 333
(Festnetz / Telekom 4,6 Cent / Minute)